UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,718	03/04/2002	Martin Hurich	10191/2275	4797

26646 7590 12/11/2007

KENYON & KENYON LLP
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
12/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/090,718	HURICH, MARTIN	
	Examiner	Art Unit	
	David García Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed September 17, 2007, have been fully considered.

2. Claims 1-19 are pending and have been examined.

Response to Amendment

3. Applicant's arguments with respect to the prior art have been considered but are moot in view of the new ground(s) of rejection.

Continued Examination Under 37 CFR 1.114

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Takaragi et al. (US Patent 6,141,421, hereinafter Takaragi).

Regarding claims 1 and 7, Takaragi teaches

- a method of data encryption in programming of a control unit comprising:

- encrypting a complete stream of data to be transmitted in a programming unit using a first key, wherein a byte by byte encryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs **(col. 5, lines 4-25, encryption and compression are performed together)**;
- transmitting the data that had been encrypted to the control unit via a data line **(col. 5, lines 4-25, encrypted and compressed message sent to receiver)**; and
- decrypting the data that had been encrypted in the programming unit using a second key provided in the control unit **(fig. 19, col. 14, lines 58-67, decoding process)**;
- wherein: successive bytes during encryption are provided with an index i, where i = 0,1,2,..., an encrypted byte n* is formed from an unencrypted byte n according to the following, a starting value n_{-1} being used for decryption and encryption **(col. 13, lines 45-67, first n bits)**:
- $n_{-1} \equiv S_0$
- $n_i^* = \left(n_i <<< \sum_{j=0}^{i} n_{j-1}^* \right) \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^* \right)}$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**
- an unencrypted byte n is formed from an encrypted byte n* according to the following:

- $n_i = \left(n_i^* \oplus S_{h\left(\sum_{j=0}^{i} n_{j-1}^*\right)} \right) >>> \sum_{j=0}^{i} n_{j-1}^*$ **(col. 9, lines 30-45, cyclically shifting bits and exclusive OR operations)**

Regarding claim 11, Takaragi teaches

- performing an encryption of a complete stream of data in accordance with a table and a hash function **(abstract, hash function)**, wherein a byte by byte encryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs **(abstract, input M, output longer)**.

Regarding claim 12, Takaragi teaches

- wherein the computing unit includes an electronic computing unit in a programming unit **(col. 6, lines 1-13, apparatus)**.

Regarding claim 19, Takaragi teaches

- wherein there is no bit-wise allocation between input and output data **(abstract, input M, output longer)**.

Regarding claim 13, Takaragi teaches

- performing a decryption of a complete stream of data in accordance with a table and a hash function **(abstract, hash function)**, wherein a byte by byte decryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs **(abstract, input M, output longer)**.

Regarding claim 14, Takaragi teaches

- wherein the computing unit includes an electronic computing unit in a control unit **(col. 6, lines 1-13, apparatus)**.

Regarding claim 15, Takaragi teaches

- a program code executable on a computing unit for performing an encryption of a complete stream of data in accordance with a table and a hash function **(abstract, hash function)**,
- wherein a byte by byte encryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs **(abstract, input M, output longer)**.

Regarding claim 16, Takaragi teaches

- a program code executable on a computing unit for performing a decryption of a complete stream of data in accordance with a table and a hash function **(abstract, hash function)**, wherein a byte by byte decryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs **(abstract, input M, output longer)**.

Regarding claims 2 and 8, Takaragi teaches wherein the first key and the second key are identical **(col. 3, lines 25-50, DES algorithm)**.

Regarding claims 3 and 9, Takaragi teaches wherein the first key and the second key are not identical **(col. 16, lines 10-20, RSA algorithm)**.

Regarding claim 4, Takaragi teaches wherein each one of the first key and the second key includes a table that is accessed by a hash function **(col. 11, lines 35-55, hash function)**.

Regarding claim 5, Takaragi teaches wherein at least one of the first key and the second key is implemented in an electronic circuit **(fig 15, 1508, random number generator)**.

Regarding claim 6, Takaragi teaches wherein at least one of the first key and the second key is implemented in the form of a computer program **(fig. 13, col. 11, lines 35-55, output of hash function is used as work key)**.

Regarding claim 10, Takaragi teaches wherein the programming unit and the control unit each includes an electronic computing unit and a memory module that are linked together by a data bus **(col. 6, lines 1-13, apparatus)**.

Regarding claims 17-18, Takaragi teaches wherein there is no bit-wise allocation between input and output data **(abstract, input M, output longer)**.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David García Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

8. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

9. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/